Utilization of Possible Security and Privacy Issues Considering the Component Interaction in High Speed Communication Networks

Reshma Ashik Chauhan

Senior Research Analyst, SMRVD Security Solutions, India.

Abstract

The Internet of Things (IoT), an evolutionary technology that raised and gained huge scope in the science and engineering applications solving problems without the intervention of human-human work force. It enables mostly smart work force i.e. creating an interaction between human to machine, machine to machine. The internet of things (IoT) enabled a common operating picture (COP) across the various applications of modern day living. The COP is achieved through the advancements seen in wireless sensor network devices that were able to communicate through the network thereby exchanging information and performing various analysis. This paper elaborates the possible security and privacy issues considering the component interaction in IoT and studies how the distributed ledger based blockchain technology contribute to it.

Keywords: Data communication; Communication Networks; Intrusion detection.

1. Introduction

The integration of all network technologies could make it complex and difficulty in handling when working on wider and large application point of view. The complex scale of device integration, network interconnection, and distributed nature of the things in IoT gives a scope for central server concept where all the things or the devices would compulsory relay on it for authentication [1-11]. In this case the interconnection between the devices would become unreliable allowing the data sharing with false authentications or allowing device spoofing leading to insecure data flow [12-17]. For clear understanding of the problem concerned with IoT, one

can refer to the views of Gartner and International Telecommunication Union reports. These two reports suggest that in future i.e. twenty billion physical things could connect to the internet and operate as a single network under IoT [18-29]. This statement suggests that IoT could be become much more complex in the coming future by connecting to a Network of Plentiful Things (NPT) making a provision for digital access. In such cases, the NPT devices could obtain enormous amount of information from the inclosing boundaries or the application or focus environment.

These devices must communicate with the network and software defined computing and analytics platform, and this process is completely done through internet and leading to a point of central server storage. This communication results in the rich interactions between the things and network IoT architecture giving a scope for huge data generation allowing the reliable and trustworthy services over the wide area network of things through the Centralized Data Management Servers (CDMS). Here, reliability and trustworthiness in providing services could not be done in fully secure manner [30-42]. Chances of security and privacy issues with the data is possible and it is due to the due to the sensitive ness of the things that are interconnected among them as well as the network.

These technologies include communication technology, information technology, electronic sensor and actuator technology, and the trending advancements in computing and analytics. The integration of all such technologies could make it complex and difficulty in handling when working on wider and large application point of view [43-51]. The complex scale of device integration, network interconnection, and distributed nature of the things in IoT gives a scope for central server concept where all the things or the devices would compulsory relay on it for authentication.

In this case the interconnection between the devices would become unreliable allowing the data sharing with false authentications or allowing device spoofing leading to insecure data flow. For clear understanding of the problem concerned

with IoT, one can refer to the views of Gartner expressed in 2016 and International Telecommunication Union reports of 2015. These two reports suggest that in future i.e. by the end of 2020, twenty billion physical things could connect to the internet and operate as a single network under IoT.

These devices must communicate with the network and software defined computing and analytics platform, and this process is completely done through internet and leading to a point of central server storage [52-64]. This communication results in the rich interactions between the things and network IoT architecture giving a scope for huge data generation allowing the reliable and trustworthy services over the wide area network of things through the Centralized Data Management Servers (CDMS).

Here, reliability and trustworthiness in providing services could not be done in fully secure manner. Chances of security and privacy issues with the data is possible and it is due to the due to the sensitive ness of the things that are interconnected among them as well as the network. More provision and chances exist for reveling the sensitive aspects of the data to outside world (outside of the communicating network or NPT) through the false authentications, device spoofing. This leads to the various security and privacy issues in IoT making it as a challenge to encounter. To address the security and privacy issues in IoT, we can eliminate centralized maintenance of the NPT produced data and thereby introducing the new Distributed Ledger -based technology called, a blockchain technology. This paper focuses on the blockchain technology in IoT by analyzing the possible data interruptions and security concerns during the IoT component interaction.

2. Challenges

Even though, IoT has several benefits and able to solve wide range of problems in various sectors, still the challenges exist. These challenges might be in the form of overcoming the security issues, privacy concerns etc. This section briefly explains the various possible issues by considering the study on the IoT component interaction.

Mostly the challenges in IoT are related to the security and privacy concerns. Apart from these, few other challenges are interoperability, lack of standards, legal challenges, regulatory issues, rights issues, emerging IoT economy issues, and other developmental issues. A report on IoT issues and challenges by The Internet Society (ISOC) prepared suggests various possible issues and how they were raised. Summary of these issues and challenges.

The resulting challenges of such issues are also stated. Here, to make it clearer on the various issues related to security and privacy aspects, IoT component interaction study is considered. Three major components of IoT are the Things with Networked Sensors and Actuators (TNSA), Raw Information and Processed Data Storage (R-IP-DS), Analytical and Computing Engines (ACE). The interaction between these three IoT components were studied briefly to point out the chances of arising security and privacy issues.

From the interaction point of view, data flow will start from the data collection unit i.e. typically some things with networked sensors and actuators to information processing and storage unit i.e. typically raw information processing and data storage in the form of report states. During this process chances of losing, mishandling of the data occurs making the data flow process not 100%.

This data must flow through the internet with some protocols and chances of misleading or misinterpret the protocols with the help of external influence is highly possible, for example, hackers can control the data process flow. During the second interaction between the R-IP-DS and ACE, the computing engines can be hacked or taken control by external users. In this case chances of analysis interruptions exists.

The third interaction is between the ACE to TNSA, here the feedback as per the computing algorithms must be sent and accordingly the things to should act. Here also chances of hacking and negative control over feedback loop is possible. Apart from interactions between these three components, in each individual component also chances of losing the data occurs by means wrong protocols. Hence, there is

huge scope for the security and privacy concerns in IoT, this even might be a serious problem in large scale IoT implementation.

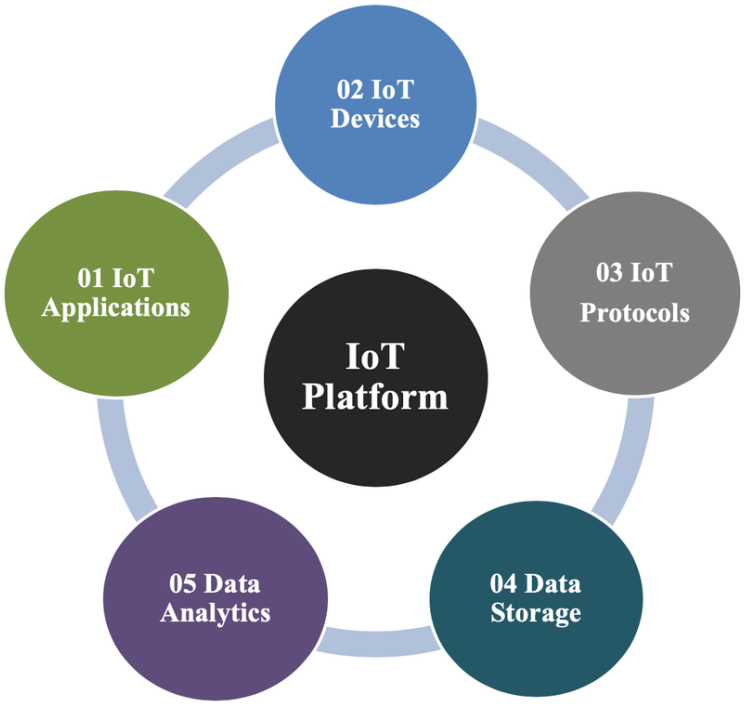

Fig. 1. Interaction of platforms

The blockchain technology would be one of the remedy for addressing the security and privacy issues in IoT. This is because, the blockchain technology eliminates the central server concept of IoT and allows the data to flow through the blockchain distributed ledger for each transaction with appropriate authentication.

3. Blockchain Technology Based Solutions

Blockchain technology evolved with the success seen in the cryptocurrency named Bitcoin. BC technology is behind the development of Bitcoin and is the key part. Blockchain is ledger-based tamper proof technology that allows various use cases in wide range of applications.

In general, the BC represents a continuously maintained and controlled database considering growing factors and collected data sample sets. The key elements of BC

are participant created transactions, and the recorder blocks of such transactions. Here, the recorder block checks whether, transaction details were maintained in the correct sequence or not. This does not allow any tampering of the data available. If the recorded data must be maintained in sequential order, the need for chain approach arises. This maintained transaction was shared with the network of participated nodes. This eliminates the concept of central server by identifying each node that is participated in the transaction sharing process by using the cryptography. This allows the secure authentication.

Blockchain technology would give better solution to the problems faced by IoT systems. In the growing scenarios of IoT systems, there are more chances for having increased number of interacting things or devices in it. These increased number of devices will try to interact with each making internet as a medium. This would lead to many hurdles because, in IoT systems, mostly the collected data is maintained in the central servers. If the devices want to access the data they have to interact using the centralized network and the data flow will happen through the central server, this process flow. But the growing needs of IoT and its applications were portraying IoT as large-scale systems with integration of advanced technologies. In such large-scale IoT systems, the centralized server will not be an effective approach.

Most of the IoT systems, that are implemented as of now are relaying on centralized server concept. In IoT systems, the sensor devices collect the information from the focused things and allow the data transmission to the central server by means of wired/wireless network refereeing as internet. From the centralized server, analytics were performed as per the user requirements and convenience. In similar, the large scale IoT system wishes to perform the analysis, processing capabilities of existing internet infrastructure may not support effectively. For handling the huge data processed in large scale IoT systems, there is a need for increasing the internet infrastructure. One best way to solve this is to have decentralized or distributed networks where “Peer-to-Peer Networking (PPN), Distributed File Sharing (DFS),

and Autonomous Device Coordination (ADC)" functions could be capable . Blockchain can carry out these three functions allowing the IoT systems to track the huge number of connected and networked devices. BC allows the IoT systems to process transactions between the devices in co-ordination. BC will enhance the privacy and reliability of IoT systems making it to be robust.

The data flow process in IoT with BC technology is different from only IoT system. In IoT with BC, the data flow is from sensors-network-router-internet-distributed blockchain-analytics-user. Here, the distributed ledger is tamper proof which does not allow in misinterpretation, wrong authentications in data. BC complexly eliminates the Single Thread Communication (STC) in IoT making the system more trust less. With the adoption of BC in IoT, the data flow will become more reliable and secure.

Blockchain technology have the following advantages for large scale IoT systems, they are as follows:

Tamper proof data

Trust less and peer to peer messaging possibility

- ✓ Robust
- ✓ Highly reliable
- ✓ More private data
- ✓ Records the historic actions
- ✓ Records data of old transactions in smart devices.
- ✓ Permits the self-directed functioning

Studies proposed a new method for managing the networked IoT devices or things in BC computing platform using the Ethereum account. Studies considered the applicability of blockchain in IoT for addressing the security and privacy concerns by considering a case study on smart home. They have discussed the applicability of

BC in IoT by considering various procedures and transactions of components in smart home tier. Similar to IoT, the blockchain technology has wider applications, and can be used in various sectors like agriculture, business, distribution, energy, food, finance, healthcare, manufacturing, and other sectors. Even though blockchain technology when integrated with IoT could overcome the privacy and reliability concerns of IoT. However, the BC technology is also having some limitations making it as a challenge. These challenges include the limitation with the ledger storage facility, limited developments in technology, lack of skilled workforce, lack of proper legal codes and standards, variations in processing speeds and time, computing capabilities, and scalability issues.

4. Conclusion

BC represents a continuously maintained and controlled database considering growing factors and collected data sample sets. The key elements of BC are participant created transactions, and the recorder blocks of such transactions. Here, the recorder block checks whether, transaction details were maintained in the correct sequence or not. This does not allow any tampering of the data available. If the recorded data must be maintained in sequential order, the need for chain approach arises. This maintained transaction was shared with the network of participated nodes This paper dealt with the various possible security and privacy issues in IoT. These were identified based on the observations in IoT component interaction. Blockchain technology is identified as one of the solutions for addressing the issues and challenges in IoT.

References

[1] Berentsen, F. Schär, The fallacy of a cashless society, in: Beer, C. and Gnan, E. and Birchler, U.W. (Hg.), Cash on Trial, SUERF Conference Proceedings, 2016.

[2] M. Vukolić, The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication, in: International Workshop on Open Problems in Network Security, Springer, 2015.

[3] Kiayias, G. Panagiotakos, Speed-security tradeoffs in blockchain protocols, in: IACR Cryptology ePrint Archive, 2015, 2015, p. 1019.

[4] P. Yeoh, Regulatory issues in blockchain technology, J. Financ. Regul. Compliance 25 (2) (2017) 196–208.

[5] Vinod Varma Vegesna (2018). "Analysis of Artificial Intelligence Techniques for Network Intrusion Detection and Intrusion Prevention for Enhanced User Privacy", Asian Journal of Applied Science and Technology, Volume 2, Issue 4, Pages 315-330, Oct-Dec 2018.

[6] Vinod Varma Vegesna (2017). "Incorporating Wireless Sensor Networks and the Internet of Things: A Hierarchical and Security-Based Analysis," International Journal of Current Engineering and Scientific Research, Volume-4, Issue-5, Pages 94-106, Available at SSRN: https://ssrn.com/abstract=4418110

[7] Hamid Ali Abed Al-Asadi, Majida Ali Abed, AL-Asadi, Zainab sabah, Baha Al-Deen, Ahmad Naser Ismail, "Fuzzy Logic approach to Recognition of Isolated Arabic Characters", International Journal of Computer Theory and Engineering, Vol. 2, No. 1, 1793-8201, February, 2010.

[8] H. A. Al-Asadi, M.H. Al-Mansoori, S. Hitam, M. I. Saripan, and M. A. Mahdi, "Particle swarm optimization on threshold exponential gain of stimulated Brillouin scattering in single mode fibers," Optics Express, vol. 19, no. 3, pp. 1842-1853, 2011.

[9] Majida Al-Asadi, Yousif A. Al-Asadi, Hamid Ali Abed Al-Asadi, "Architectural Analysis of Multi-Agents Educational Model in Web-Learning Environments," Journal of Emerging Trends in Computing and Information Sciences, Vol. 3, No. 6, 2012.

[10] Vinod Varma Vegesna (2016). "Threat and Risk Assessment Techniques and Mitigation Approaches for Enhancing Security in Automotive Domain," International Journal of Management, Technology And Engineering, Volume VI, Issue II, July-Dec 2016, Pages 314-331.

[11] Vinod Varma Vegesna (2015). "Incorporating Data Mining Approaches and Knowledge Discovery Process to Cloud Computing for Maximizing Security," International Journal of Current Engineering and Scientific Research, Volume-2, Issue-6, Pages 118-133, Available at SSRN: https://ssrn.com/abstract=4418107

[12] R. Grosse, Bank regulation, governance and the crisis: a behavioral finance view, J. Financ. Regul. Compliance 20 (1) (2012) 4–25.

[13] M. Pilkington, 11 blockchain technology: principles and applications, in: Research Handbook on Digital Transformations, 2016, p. 225.

[14] K. Wüst, A. Gervais, Do you need a Blockchain? in: IACR Cryptology ePrint Archive, 2017, 2017, p. 375.

[15] S. Apte, N. Petrovsky, Will blockchain technology revolutionize excipient supply chain management? J. Excip. Food Chem. 7 (3) (2016) 910.

[16] K. Peterson, et al., A blockchain-based approach to health information exchange networks, in Proc. NIST Workshop Blockchain Healthcare, 2016.

[17] Vinod Varma Vegesna (2023). "Adopting a Conceptual Architecture to Mitigate an IoT Zero-Day Threat that Might Result in a Zero-Day Attack with Regard to Operational Costs and Communication Overheads," International Journal of Current Engineering and Scientific Research, Volume-10, Issue-1, Pages 9-17.

[18] Vinod Varma Vegesna (2023). "Methodology for Mitigating the Security Issues and Challenges in the Internet of Things (IoT) Framework for Enhanced Security," Asian Journal of Basic Science & Research, Vol. 5, No. 1, January-March 2023, Pages 85–102, doi: 10.38177/ajbsr.2023.5110.

[19] Hamid Ali Abed Al-Asadi and et al., "A Network Analysis for Finding the Shortest Path in Hospital Information System with GIS and GPS, Journal of Network Computing and Applications (2020) 5: 10-22.

[20] Hamid Ali Abed Al-Asadi, et al., "Nature Inspired Algorithms multi-objective histogram equalization for Grey image enhancement", Advances in Computer, Signals and Systems (2020) 4: 36-46 Clausius Scientific Press, Canada DOI: 10.23977/acss.2020.040106.

[21] Hamid Ali Abed Al-Asadi and et al., " Critical Comparative Review of Nature-Inspired Optimization Algorithms (NIOAs), International Journal of Simulation: Systems, Science and Technology (IJSSST), 2020, 21(3), PP1-15

[22] Hamid Ali Abed Al-Asadi, (2022) "1st Edition: Privacy and Security Challenges in Cloud Computing A Holistic Approach" Intelligent Internet of Things for Smart Healthcare Systems, Scopus, Taylor @Francis, CRC Press. (Book Chapter: Enhanced Hybrid and Highly Secure Cryptosystem for Mitigating Security Issues in Cloud Environments), March 2022.

[23] Vinod Varma Vegesna (2023). "Secure and Reliable Designs for Intrusion Detection Methods Developed Utilizing Artificial Intelligence Approaches," International Journal of Current Engineering and Scientific Research, Volume-10, Issue-3, Pages 1-7.

[24] Vinod Varma Vegesna (2023). "A Critical Investigation and Analysis of Strategic Techniques Before Approving Cloud Computing Service Frameworks," International Journal of Management, Technology and Engineering, Volume XIII, Issue IV, April 2023, Pages 132-144.

[25] D.C. Mills, et al., Distributed ledger technology in payments, clearing, and settlement, 2016.

[26] E. Vasilomanolakis, et al., On the security and privacy of internet of things architectures and systems, in: Secure Internet of Things (SIoT), 2015 International Workshop on, IEEE, 2015.

[27] Y. Sompolinsky, A. Zohar, Secure high-rate transaction processing in bitcoin, in: International Conference on Financial Cryptography and Data Security, 2015.

[28] U. Uko, Before you invest in cryptocurrency: A simple guide to understanding the cryptocurrency market, blockchain, mining, bitcoin, exchanges, Ethereum, Ripple etc., 2018.

[29] P. Tasatanattakool, C. Techapanupreeda, Blockchain: Challenges and applications, in: Information Networking (ICOIN), 2018 International Conference on, IEEE, 2018.

[30] M. Spearpoint, A proposed currency system for academic peer review payments using the blockchain technology, Publications 5 (3) (2017) 19.

[31] Vinod Varma Vegesna (2022). “Utilising VAPT Technologies (Vulnerability Assessment & Penetration Testing) as a Method for Actively Preventing Cyberattacks,” International Journal of Management, Technology and Engineering, Volume XII, Issue VII, July 2022, Pages 81-94.

[32] Hamzah F. Zmezm, Hareth Zmezm, Mustafa S.Khalefa, Hamid Ali Abed Al-Asadi, "A Novel Scan2Pass Architecture for Enhancing Security towards E-Commerce," Future Technologies Conference 2017, 29-30 November 2017 | Vancouver, BC, Canada, 2017.

[33] Hamid Ali Abed Al-Asadi, Majida Ali Al-Asadi, Nada Ali Noori , "Optimization Noise Figure of Fiber Raman Amplifier based on Bat Algorithm in Optical Communication network," International Journal of Engineering & Technology, Scopus, Vol 7, No 2, pp. 874-879, 2018.

[34] Hareth Zmezm, Mustafa S.Khalefa, Hamid Ali Abed Al-Asadi, Hamzah F. Zmezm, Dr. Hussain Falih Mahdi, Hassan Muhsen Abdulkareem Al-Haidari. "Suggested Mechanisms for Understanding the Ideas in Authentication System," International Journal of Advancements in Computing Technology9(3):10-24, 2018.

[35] Hamid Ali Abed Al-Asadi and et al., “Priority Incorporated Zone Based Distributed Clustering Algorithm For Heterogeneous Wireless Sensor Network”, Advances in Science, Technology and Engineering Systems Journal Vol. 4, No. 5, PP. 306-313, 2019.

[36] Vinod Varma Vegesna (2022). “Accelerate the development of a business without losing privacy with the help of API Security Best Practises - Enabling businesses to create more dynamic applications,” International Journal of Management, Technology and Engineering, Volume XII, Issue IX, September 2022, Pages 91-99.

[37] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2008.

[38] Kewell, R. Adams, G. Parry, Blockchain for good? Strateg. Change 26 (5) (2017) 429–437.

[39] S. Underwood, Blockchain beyond bitcoin, Commun. ACM 59 (11) (2016) 15–17.

[40] S. Singh, Y.-S. Jeong, J.H. Park, A survey on cloud computing security: Issues, threats, and solutions, J. Netw. Comput. Appl. 75 (2016) 200–222.

[41] Vinod Varma Vegesna (2022). "Using Distributed Ledger Based Blockchain Technological Advances to Address IoT Safety and Confidentiality Issues," International Journal of Current Engineering and Scientific Research, Volume-9, Issue-3, Pages 89-98.

[42] Vinod Varma Vegesna (2022). "Methodologies for Enhancing Data Integrity and Security in Distributed Cloud Computing with Techniques to Implement Security Solutions," Asian Journal of Applied Science and Technology, Volume 6, Issue 2, Pages 167-180, April-June 2022, doi: 10.38177/ajast.2022.6217.

[43] J.H. Park, J.H. Park, Blockchain security in cloud computing: Use cases, challenges, and solutions, Symmetry 9 (8) (2017) 164.

[44] K. Rehiman, S. Veni, Privacy and trust for smart mobile devices in internet of things—A literature study, Int. J. Adv. Res. Comput. Eng. Technol. 4 (5) (2015) 1775–1779.

[45] T. Xu, J.B. Wendt, M. Potkonjak, Security of IoT systems: Design challenges and opportunities, in: Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design, IEEE Press, 2014.

[46] A.G. Abbasi, Z. Khan, VeidBlock: Verifiable identity using blockchain and ledger in a software defined network, in: Companion Proceedings of The 10th International Conference on Utility and Cloud Computing, ACM, 2017.

[47] Vinod Varma Vegesna (2022). "Investigations on Cybersecurity Challenges and Mitigation Strategies in Intelligent transport systems," Irish Interdisciplinary Journal of Science and Research, Vol. 6, Iss. 4, Pages 70-86, October-December 2022, doi: 10.46759/iijsr.2022.6409.

[48] Majda Ali Abed and Hamid Ali Abed Al-Asadi, "Simplifying Handwritten Characters Recognition Using a Particle Swarm Optimization Approach", European Academic Research, Vol 1,pp. 535- 552, Issue(5), 5. 2013.

[49] Majda Ali Abed and Hamid Ali Abed Al-Asadi, "High Accuracy Arabic Handwritten Characters Recognition using (EBPANN) Architecture," International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 6 Issue 2, 2015.

[50] Hamid Ali Abed Al-Asadi and Majda Ali Abed, "Object Recognition Using Artificial Fish Swarm Algorithm on Fourier Descriptors," American Journal of Engineering, Technology and Society; Volume 2, Issue 5: pp. 105-110, 2015.

[51] Vinod Varma Vegesna (2021). "Analysis of Data Confidentiality Methods in Cloud Computing for Attaining Enhanced Security in Cloud Storage," Middle East Journal of Applied Science & Technology, Vol. 4, Iss. 2, Pages 163-178, April-June 2021, Available at SSRN: https://ssrn.com/abstract=4418127

[52] Vinod Varma Vegesna (2021). "A Highly Efficient and Secure Procedure for Protecting Privacy in Cloud Data Storage Environments," International Journal of Management, Technology and Engineering, Volume XI, Issue VII, July 2021, Pages 277-287.

[53] D.W. Kravitz, J. Cooper, Securing user identity and transactions symbiotically: IoT meets blockchain, in: Global Internet of Things Summit, GIoTS, 2017, IEEE, 2017.

[54] A. Dorri, S.S. Kanhere, R. Jurdak, Towards an optimized blockchain for IoT, in: Proceedings of the Second International Conference on Internet-of-Things Design and Implementation, ACM, 2017.

[55] M. Atzori, Blockchain technology and decentralized governance: Is the state still necessary? 2015.

[56] N. Fabiano, The internet of things ecosystem: The blockchain and privacy issues, The challenge for a global privacy standard, in: Internet of Things for the Global Community (IoTGC), 2017 International Conference on, IEEE, 2017.

[57] C.B. Technologies, Cross border technologies: International technology licensing, sales and services, 5/31/2018, 2018.

[58] Vinod Varma Vegesna (2021). "The Utilization of Information Systems for Supply Chain Management for Multicomponent Productivity Based on Cloud Computing," International Journal of Management, Technology and Engineering, Volume XI, Issue IX, September 2021, Pages 98-113.

[59] Vinod Varma Vegesna (2021). "The Applicability of Various Cyber Security Services for the Prevention of Attacks on Smart Homes," International Journal of Current Engineering and Scientific Research, Volume-8, Issue-12, Pages 14-21.

[60] Vinod Varma Vegesna (2020). "Secure and Privacy-Based Data Sharing Approaches in Cloud Computing for Healthcare Applications," Mediterranean Journal of Basic and Applied Sciences, Volume 4, Issue 4, Pages 194-209, October-December 2020, doi: 10.46382/mjbas.2020.4409.

[61] Vinod Varma Vegesna (2019). "Investigations on Different Security Techniques for Data Protection in Cloud Computing using Cryptography Schemes", Indo-Iranian Journal of Scientific Research, Volume 3, Issue 1, Pages 69-84, January-March 2019, Available at SSRN: https://ssrn.com/abstract=4418119

[62] Norta, Creation of smart-contracting collaborations for decentralized autonomous organizations, in: International Conference on Business Informatics Research, Springer, 2015.

[63] W. Reijers, F. O'Brolcháin, P. Haynes, Governance in blockchain technologies & social contract theories, Ledger 1 (2016) 134–151.

[64] A. Collomb, K. Sok, Blockchain/distributed ledger technology (DLT): What impact on the financial sector? Digi World Econ. J. (2016) 103.